UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,046	07/12/2001	Christine Cheng	2043.258US1	3861

49845 7590 03/25/2009

SCHWEGMAN, LUNDBERG & WOESSNER/EBAY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
OYEBISI, OJO O	
ART UNIT	PAPER NUMBER
3696	

NOTIFICATION DATE	DELIVERY MODE
03/25/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@SLWIP.COM

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/905,046
Filing Date: July 12, 2001
Appellant(s): CHENG ET AL.

Charles E. Steffey
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/04/2008 appealing from the Office action mailed on 02/14/08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,919,257	**Trostle**	**7-1999**
5,557,742	**Smaha et al**	**9-1996**

Buchner et al (Buchner hereinafter, Discovering Internet marketing intelligence through online analytical web usage mining, ACM SIGMOD Record archive, Volume 27, Issue 4 (December 1998), Pages: 54 – 61, Year of Publication: 1998, ISSN:0163-5808).

Miller (Michael Miller, The complete Idiot's Guide to Ebay Online Auctions, copyright July 1999).

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-6, 31-36, and 40 are rejected under 35 U.S.C. 102(b) as being anticipated by Trostle (US PAT: 5,919,257).

Re claims 1 and 2. Trostle teaches a method to detect fraudulent activities at a network-based transaction facility, the method comprising: causing a first identifier (i.e., authorized username) associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction

facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and detecting a potentially fraudulent activity by detecting a lack of correspondence (i.e., In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends, see col.5 lines 45-55) between the first identifier stored on the machine and a second identifier (i.e., entered username) associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88. The encrypted private key can only be decrypted with the user's password. In step 90 the server checks if any login restrictions, such as, time restrictions, station restrictions and account lock-out restrictions have been violated. These restrictions prevent logins from unauthorized workstations or logins during the wrong time of day. If there are violations, access is denied (step 86). However, if there are no login restrictions, the user is prompted to enter a password in step 92 and the validity of the password is determined in step 94, see col.5 lines 45-67).

Re claims 31-33, and 40. Claims 31-33, and 40 recite similar limitations to claim 1 and thus rejected using the same art and rationale as in the rejection of claim 1 supra.

Re claims 3 and 34. Trostle discloses a method comprising causing the lack of correspondence between the first identifier and second identifier to be detected at the machine (i.e., In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends, see col.5 lines 45-55).

Re claims 4-6, 35-36. Trostle further discloses a method comprising receiving both the first identifier and the second identifier at the network-based transaction facility from the machine, and detecting the lack of correspondence between the first identifier and second identifier at the network-based transaction facility (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88, see col.5 lines 45-60).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 7-8, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Buchner et al (Buchner hereinafter, Discovering Internet marketing intelligence through online analytical web usage mining, ACM SIGMOD Record archive, Volume 27, Issue 4 (December 1998), Pages: 54 – 61, Year of Publication: 1998, ISSN:0163-5808).

Re claims 7-8, and 37. Trostle does not explicitly disclose a method comprising causing the first and second identifier to be stored on the machine within a cookie. However, Buchner makes this disclosure (i.e., cookies are tokens generated by the web server and held by the clients. The information stored in a cookie log helps to ameliorate the transactionless state of the web server interactions……., the logged cookie data is customizable, which goes hand in hand with the structure and the content of the marketing data, ……the logged query data must be linked to the access log through cookie data and or/registration data (i.e., identifiers), see pg 55 col.2 paragraphs 2 and 3). Thus it would have been obvious to one of ordinary skill in the art to combine the teachings of Buchner and Trostle to enable servers to track client access across their hosted web pages. Further, storing user identifiers on the machine within a cookie is a well-known cookie bundling scheme. Cookie bundling is a common practice wherein all of the separate cookies pertaining to different type of user transaction preferences are packed together into one file. Thus it would have been obvious to one of ordinary skill in the art to introduce the well-known scheme in Trostle to enable separate cookies

pertaining to different type of user transaction preferences to be packed together into one file.

5. Claims 9-19, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Buchner as applied to claims 8 and 37 above, and further in view of Miller (Michael Miller, The complete Idiot's Guide to Ebay Online Auctions, copyright July 1999).

Re claims 9, 10. Neither Trostle nor Buchner explicitly discloses a method wherein the first sales-related event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility. However, Miller discloses a method wherein the first event includes one of registering with the network-based transaction facility (see pg 133), communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility (i.e., ebay, see pg 52) communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility (i.e., ebay feedback, see pgs 157-161). Thus it would have been obvious to incorporate what is taught by Miller into the combination of Trostle and Buchner to allow individuals and small businesses to sell and buy items from other internet users worldwide.

Re claims 11-14, and 38. Trostle discloses the method comprising: the detection of the lack of correspondence between the first identifier and the second identifier at one of the machine and the network-based transaction facility; inspect for the potentially fraudulent activity (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88, see col.5 lines 45-60), and causing the potentially fraudulent activity to be recorded into a database. (i.e., If the values are equal then illicit changes have not been made to the selected executables programs, and execution continues with step 90 which returns workstation execution to the system BIOS. Otherwise, step 92 is performed to notify the user, and/or the network system administrator, that an unauthorized change has been detected. The workstation may also make an entry in an **audit server audit log,** see col.7 lines 27-38). Trostle does not explicitly disclose causing the first identifier and the second identifier to be stored on the machine within a shill cookie; causing a cookie identifier to be stored within the shill cookie; causing the shill cookie to be coupled to a cookie bundle which records a plurality of transaction preferences for the first user identity and the second user identity on the machine; causing the shill cookie bundle to be sent from the machine to the network-based transaction facility when the second user identify makes the second sales transaction event with the network-based transaction facility using the machine;

causing the shill cookie to be appended with the second identifier. However, Buchner makes this disclosure (i.e., cookies are tokens generated by the web server and held by the clients. The information stored in a cookie log helps to ameliorate the transactionless state of the web server interactions……., the logged cookie data is customizable, which goes hand in hand with the structure and the content of the marketing data, ……the logged query data must be linked to the access log through cookie data and or/registration data (i.e., identifiers). Thus it would have been obvious to one of ordinary skill in the art to combine the teachings of Trostle and Buchner to enable servers to track client access across their hosted web pages. Further, storing user identifiers on the machine within a cookie is a well-known cookie bundling scheme. Cookie bundling is a common practice wherein all of the separate cookies pertaining to different type of user transaction preferences are packed together into one file. Thus it would have been obvious to one of ordinary skill in the art to introduce the well-known scheme in Trostle to enable separate cookies pertaining to different type of user transaction preferences to be packed together into one file.

Re claim 15. Trostle discloses a method wherein the machine comprises a computer connected to the network-based transaction facility (i.e., a networked workstation performs an intrusion detection hashing function on selected workstation executable programs, see abstract).

Re claim 16. Neither Trostle nor Buchner discloses a method wherein the network-based transaction facility comprises an Internet-based auction facility. However Miller makes this disclosure (i.e., ebay, see pg 52). Thus it would have been obvious to

incorporate what is taught by Miller into combination of Trostle and Buchner to allow individuals and small businesses to sell items to sell and buy items from other internet users worldwide.

Re claims 17, 18-19. Trostle does not explicitly disclose a method as in claim 16 further comprising: causing the shill cookie to record and to store a predetermined number of user identifiers. However, Buchner makes this disclosure (i.e., cookies are tokens generated by the web server and held by the clients. The information stored in a cookie log helps to ameliorate the transactionless state of the web server interactions……., the logged cookie data is customizable, which goes hand in hand with the structure and the content of the marketing data, ……the logged query data must be linked to the access log through cookie data and or/registration data (i.e., identifiers). Thus it would have been obvious to one of ordinary skill in the art to combine the teachings of Trostle and Buchner to enable servers to track client access across their hosted web pages. Further, storing user identifiers on the machine within a cookie is a well-known cookie bundling scheme. Cookie bundling is a common practice wherein all of the separate cookies pertaining to different type of user transaction preferences are packed together into one file. Thus it would have been obvious to one of ordinary skill in the art to introduce the well-known scheme in Trostle to enable separate cookies pertaining to different type of user transaction preferences to be packed together into one file.

6. Claims 20-30, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Buchner and Miller as applied to claims 19 and 38 above and further in view of Smaha et al (Smaha hereinafter, US PAT: 5,557,742).

Re claims 20-21, and 39. Neither Trostle nor combination of Buchner and Miller explicitly discloses a method further comprising: generating a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field; recording each of the potentially fraudulent activities and corresponding information into the potential fraudulent activities table; updating the potential fraudulent activities table at least on a periodic basis; and providing an updated report of the potential fraudulent activities table to an investigation team. However, Smaha discloses generating a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field (i.e., generate misuse report and load pres-elected fields, see fig.6B element 170 and element 176); recording each of the potentially fraudulent activities (i.e., misuse) and corresponding information into the potential fraudulent activities table (see fig.4 element 126); updating the potential fraudulent activities table at least on a periodic basis (i.e., once a misuse has been detected, an output mechanism generates a signal for use by notification and storage mechanism, see col.3 lines 40-45, also see col.6 lines 11-14); and providing an updated report of the potential fraudulent activities table to an investigation team (i.e., the detection system then generates a text-based output report for a user to view or stored, see col.3 lines 40-44). Thus it would have been obvious to one of ordinary skill in the art to combine Trostle, Buchner, Miller and Smaha to enable a user to store, view and analyze the fraudulent activities.

Re claim 22. Neither Trostle nor Buchner explicitly discloses a method wherein the new event includes one of registering with the network-based transaction facility,

communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility. However, Miller discloses a method wherein the new event includes one of registering with the network-based transaction facility (see pg 133), communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility (i.e., ebay, see pg 52) communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility (i.e., ebay feedback, see pgs 157-161). Thus it would have been obvious to incorporate what is taught by Miller into the combination of Trostle and Buchner to allow individuals and small businesses to sell and buy items from other internet users worldwide.

Re claims 23 and 24. Neither Trostle nor combination of Buchner and Miller discloses a method comprising providing the updated report to the investigation team at a predetermined time. However, Shama discloses providing the updated report to the investigation team (i.e., a user) at a predetermined time (i.e., the detection system then generates a text-based output report for a user to view or stored, see col.3 lines 40-44). Thus it would have been obvious to one of ordinary skill in the art to combine Trostle, Buchner, Miller and Smaha to enable a user to store, view and analyze the fraudulent activities.

Re claim 25. Neither Trostle nor the combination of Buchner, Miller and Shama

discloses a method further comprising providing a priority ranking system having a low priority for a low potential fraudulent activity frequency, a medium priority for a medium potential fraudulent activity frequency and a high priority for a high potential fraudulent activity frequency. However, it is old and well in business management art to prioritize events based on the events degree of importance. Thus it would have been obvious to one of ordinary skill in the art to incorporate what is old and well known in the art into the combination of Trostle, Buchner, Miller and Shama to prioritize the frequency of fraudulent activities and to enable the system to process data more efficiently.

Re claim 26. Trostle discloses a method further comprising examining the updated report to confirm the potentially fraudulent activity (i.e., the detection system then generates a text-based output report for a user to view or stored, see col.3 lines 40-44).

Re claim 27. Trostle discloses how fraudulent activities i.e., an authorized change to a workstation can be detected and prevented. Neither Trostle nor Buchner explicitly discloses a method wherein the potentially fraudulent activity includes one of shill biddings and shill feedbacks. However, Miller explicitly disclose a method wherein the potentially fraudulent activity includes one of shill biddings and shill feedbacks (see pg 218 and pg 222). Thus it would have been obvious to one of ordinary skill in the art to use the intrusion detection system of Trostle to detect and prevent fraudulent activities in online auction market i.e., shill bidding and shill feedback as taught by Miller.

Re claim 28. Neither Trostle nor the combination of Buchner and Miller discloses a method wherein the recording does not affect any one of the first sales related event, the second sales event, and the new event. However Smaha makes this disclosure (i.e.,

a method for using processing system inputs to form events, processing the events by the misuse engine according to a set of selectable misuses, and generating one or more misuse outputs. The method converts system-generated inputs to events by establishing a first data structure for use by the system which stores the event. The data structure has elements including (1) authentication information; (2) subject information; and (3) object information. The method further extracts from system audit trail records, system log file data, and system security state data the information necessary for the first data structure. The method includes the steps of storing the events into the first data structure, see col.12 line 65 – col.13 line10). Thus it would have been obvious to combine the teachings of Trostle, Buchner, Miller and Smaha to detect and prevent fraudulent activities in online auction market.

Re claim 29. Trostle further discloses a method further comprising causing the detection of the potentially fraudulent activity responsive a matching of at least two user transaction preferences from at least two different user identifies (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88. The encrypted private key can only be decrypted with the user's password. In step 90 the server checks if any login restrictions, such as, time restrictions, station restrictions and account lock-out restrictions have been violated. These restrictions

prevent logins from unauthorized workstations or logins during the wrong time of day. If there are violations, access is denied (step 86). However, if there are no login restrictions, the user is prompted to enter a password in step 92 and the validity of the password is determined in step 94, see col.5 lines 45-67).

Re claim 30. Neither Trostle nor Buchner discloses a method wherein the user transaction preferences comprise credit card numbers, bidding histories, payment methods, and shipping addresses. However, Miller makes this disclosure (see pg 23). Thus it would have been obvious to one of ordinary skill in the art to combine the teachings of Trostle, Buchner and Miller to detect and prevent fraudulent activities in online auction market.

(10) Response to Argument

In response to the appellant's argument concerning the rejections of claims 1-6, 31-36 and 40 under 35 U.S.C 102 (b).

The appellant argues in substance that the primary reference, Trostle, fails to teach the limitations: detecting a potentially fraudulent activity by detecting the lack of correspondence between a first identifier stored on a machine and a second identifier; and storing a first user identity responsive to a first sales-related event with respect to the network-based transaction facility, as recited in claim 1. Contrary to the appellant's assertion, Trostle discloses in col.5 lines 45-67 i.e., " in step 82, a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and

the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88. The encrypted private key can only be decrypted with the user's password. In step 90 the server checks if any login restrictions, such as, time restrictions, station restrictions and account lock-out restrictions have been violated. These restrictions prevent logins from unauthorized workstations or logins during the wrong time of day. If there are violations, access is denied (step 86). However, if there are no login restrictions, the user is prompted to enter a password in step 92 and the validity of the password is determined in step 94." Clearly, in col.5 lines 45-67, Trostle is describing an authentication process wherein a user identity (i.e., username) is compared to pre-stored user information, and if a match is not found between the entered username and the pre-stored information, network access is denied to the said user, and the log-in process terminates. Thus, the examiner perceives the authentication process described by Trostle in col.5 lines 45-67 to constitute the appellant's claimed limitations i.e., "storing a first user identity responsive to a first sales-related event with respect to the network-based transaction facility; detecting a potentially fraudulent activity by detecting the lack of correspondence between a first identifier stored on a machine and a second identifier." All in all, the authentication process disclosed by Trostle supra reads on these limitations. The examiner contends that the pre-stored username and the entered username constitute appellant claimed first user identity and second user identity. In Trostle, the entered username is matched/compared to the prestored username to detect correspondence. If the two identities or identifiers match the user is

allowed to proceed but if the two identifiers do not match, then user is denied access. Thus this authentication process as described by Trostle supra constitutes appellant's claimed limitation of detecting the lack of correspondence between a first identifier stored on a machine and a second identifier.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/OJO O OYEBISI/

Examiner, Art Unit 3696

Conferees:

/THOMAS A DIXON/

Supervisory Patent Examiner, Art Unit 3696

Vincent Millin /vm/
Appeal Practice Specialist, Technology Center 3600